PERANGKAT LUNAK UNTUK PROSES ENKRIPSI DESKRIPSI MESSAGE EMAIL DENGAN ALGORITMA BLOWFISH

Ary Fathany Kristiawan[1)] **Rudy Setiawan**[2)]

1) Program Studi Sistem Informasi, STIKOM Surabaya, email: fathany@hackersclub.net
2) Program Studi Sistem Informasi, STIKOM Surabaya, email: rudy@stikom.edu

Abstract: Alots of people use email fiture in internet, bring about individually reading data email prevent from other person to read without any permission include in Dwi Rejeki Abadai Company. To overcome this problem it needs some application to help user in security. Encription process using Blowfish Algorithm can increase email security to prevent some one without any permission reading the email.

Keywords: Email, Encription, Description, Blowfish, Security

Dunia komputer berkembang pesat saat ini, bukan hanya dinegara maju, dinegara berkembangpun terjadi peningkatan terhadap penggunaan komputer baik dalam aktifitas bisnis, pendidikan, dan bidang-bidang yang lain. Salah satu perkembangan komputer yang cukup pesat di Indonesia akhir-akhir ini adalah penggunaan internet.

Salah satu fitur internet yang banyak dimanfaatkan adalah email atau surat elektronik. Karena banyaknya pengguna internet di Indonesia yang tidak menggunakan komputer milik pribadi, menyebabkan terjadinya pembacaan data email yang sifatnya pribadi oleh pihak yang lain yang tidak berhak, hal ini terjadi karena cara kerja email yang harus melewati beberapa server sebelum sampai ke alamat yang dituju (Kurniawan, 2002). Untuk mengatasi masalah tersebut, peneliti tertarik membuat sebuah program dengan metode enkripsi terhadap isi suatu email sehingga dapat meningkatkan keamanan email dari pembacaan oleh pihak-pihak yang tidak berhak.

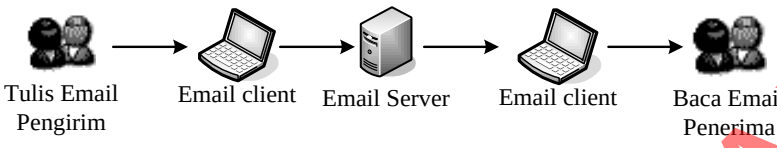
Teknik-teknik yang digunakan dalam enkripsi email telah berkembang pesat dan sebagian dari teknik-teknik tersebut sudah menjadi standar internasional. Selain Blowfish terdapat teknik algoritma enkripsi yang cukup terkenal antara lain *Data Encryption Standart*(DES), Tripe DES, *International Data Encryption Algorithm*(IDEA), dan RC5. Algoritma diatas telah banyak digunakan untuk perangkat lunak enkripsi, salah satu yang terkenal adalah *Pretty Good Privacy*(PGP) (Stiawan, 2005).

Permasalahan penelitian yang dihadapi adalah bagaimana membuat perangkat lunak untuk mengenkripsi isi suatu email menggunakan algoritma Blowfish dengan memanfaatkan sebuah kunci yang nantinya digunakan lagi untuk mendekripsinya sehingga email terbentuk seperti asalnya. Tujuan dari penelitian ini adalah bagaimana mengimplementasikan algoritma Blowfish untuk mengenkripsi isi dari suatu email dan mendekripsinya kembali sehingga kebentuk aslinya yang benar.

Email adalah salah satu layanan yang sangat populer saat ini yang berguna untuk sarana kirim mengirim pesan selayaknya surat melalui jalur internet, protokol yang digunakan untuk mengirim email adalah SMTP (*Simple Mail*

Transport Protocol), sedangkan untuk men-download email digunakan protokol POP (*Post Office Protocol*) atau IMAP (*Internet Message Access Protocol*) (Sembiring, 2002).

Untuk mengirim email diperlukan suatu program email client. email yang dikirim melalui beberapa point sebelum sampai di tujuan. Untuk lebih detail dapat diuraikan pada gambar 1.



Gambar 1. Metode Pengiriman Email

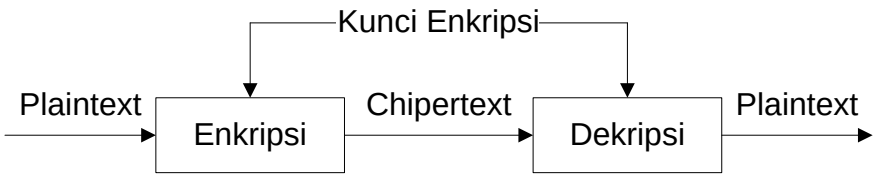
Terlihat email yang terkirim hanya melalui 3 point (selain komputer pengirim dan penerima). Sebenarnya lebih dari itu sebab setelah email meninggalkan POP3 Server maka itu akan melalui banyak server-server lainnya. Tidak tertutup kemungkinan email yang dikirim disadap orang lain. Maka dari itu bila email yang dikirim mengandung isi yang sensitif sebaiknya dilakukan tindakan pencegahan, dengan mengacak (enkrip) data dalam email tersebut (contohnya menggunakan PGP, sertifikat digital, dsb.) (Wikipedia, 2005).

Keamanan data email anda tidak terjamin. email anda terbuka untuk umum, dalam artian semua isinya dapat dibaca oleh orang lain sebab email yang terkirim akan melewati banyak server sebelum sampai di tujuan. Tidak tertutup kemungkinan ada orang usil lalu menyadap email anda (Wikipedia, 2005). Pada dasarnya tidak sulit untuk menghadang email karena secara umum pada paket data yang dilewatkan pada jaringan tidak dilakukan enkripsi. Ini berbeda jika digunakan metode enkapsulasi (pembungkusan) atau menggunakan suatu metode enkripsi. Ada banyak perangkat lunak yang dapat digunakan untuk menangkap dan membaca paket email, salah satunya adalah mailsnarf yang terdapat pada *utility dsniff*. Mailsnarf menghadang suatu email utuh. Cara ini dikenal dengan istilah *Snife*.

Enkripsi adalah sebuah proses di mana sebuah pesan (plaintext) ditransformasikan ke bentuk pesan lain (chipertext) menggunakan fungsi metematis dan sebuah enkripsi password spesial yang dikenal dengan istilah key. Dekripsi merupakan proses kebalikannya di mana chipertext ditransformasikan kembali ke plaintext dengan metode matematis dan menggunakan suatu key. Dalam membahas model-model enkripsi dijelaskan dua hal yang penting, yaitu enkripsi dengan kunci simetris dan enkripsi dengan kunci asimetris (Stiawan, 2005).

Enkripsi dengan Kunci Simetris seperti pada gambar 2. dilakukan jika pengirim dan penerima telah sepakat untuk menggunakan metode enkripsi atau kunci kunci enkripsi tertentu. Metode enkripsi atau kuncinya ini harus dijaga ketat supaya tidak ada pihak luar yang mengetahuinya. Masalahnya sekarang adalah bagaimana memberitahukan pihak penerima mengenai metode atau kunci yang akan dipakai sebelum komunikasi yang aman bisa berlangsung. Kesepakatan ini

dapat dicapai lewat jalur komunikasi lain, misalkan bertemu langsung atau media lain (telepon atau lainnya).

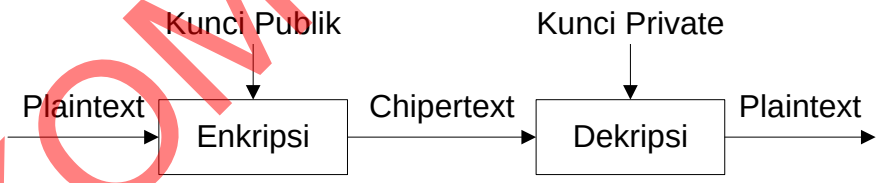


Gambar 2. Enkripsi Kunci Simetris

Ada beberapa algoritma enkripsi yang termasuk dalam golongan ini, diantaranya DES, Triple DES, IDEA, Blowfish (Stiawan, 2005).

Enkripsi dengan Kunci Asimetris (Publik) pada gambar 3. menggunakan kunci yang perlu diketahui oleh umum, atau kunci publik yang dimiliki dapat disebarkan ke orang lain. Jika teknik kriptografi menggunakan kunci simetris memakai kunci yang sama untuk melakukan proses enkripsi dan dekripsi, teknik kriptografi ini menggunakan kunci asimetris yang memerlukan sepasang kunci untuk enkripsi dan dekripsi.

Pesan yang dienkripsi menggunakan sebuah kunci hanya bisa dibuka menggunakan kunci pasangannya. Pesan tersebut tidak bisa dibuka menggunakan kunci yang sama. Kunci yang pertama disebut kunci publik dan kunci pasangannya disebut kunci private. Jadi, sebuah pesan yang dienkripsi menggunakan kunci publik hanya bisa dibuka menggunakan kunci private, demikian pula sebaliknya. Proses enkripsi atau dekripsi tersebut hanya bisa dilakukan menggunakan pasangan kunci yang tepat. Jika pasangan kuncinya salah, proses enkripsi atau dekripsi akan gagal. Kunci publik dapat diketahui oleh semua orang, sedangkan kunci private hanya boleh diketahui oleh satu orang saja, yaitu orang yang berhak memilikinya.



Gambar 3. Enkripsi Kunci Publik

Ada beberapa algoritma enkripsi yang terkenal misalnya, *sistem Diffie Hellman*, RSA, dan PGP (Stiawan, 2005).

Algoritma Blowfish pada dasarnya terdiri dari dua bagian yaitu *key expansion* dan enkripsi data, *key expansion* merubah kunci yang dapat mencapai 448 bit menjadi beberapa array subkunci (*subkey*) dengan total 4168 byte, sedangkan enkripsi data terdiri dari iterasi fungsi sederhana sebanyak 16 kali, setiap putaran terdiri dari permutasi kunci-*dependent* dan subtitusi kunci dan data –*dependent*, semua operasi adalah penambahan dan XOR pada variabel 32 bit. XOR (*exclusive-or* digambarkan dengan simbol ⊕) akan bernilai benar jika salah satu operasinya bernilai benar, dan yang lainnya akan bernilai salah. Blowfish menggunakan subkunci yang besar, kunci ini harus dihitung sebelum proses

enkripsi atau dekripsi data. Subkunci dihitung menggunakan algoritma Blowfish dan algoritmanya adalah sebagai berikut :

Inisialisasi P-array dan kemudian empat S-box secara berurutan seperti pada gambar 4 dengan string yang tetap, string ini terdiri dari digit hexadecimal dari pi. Array P terdiri dari delapan belas 32 bit subkunci:

$P_1,P_2,P_3,\ldots,P_{18}$

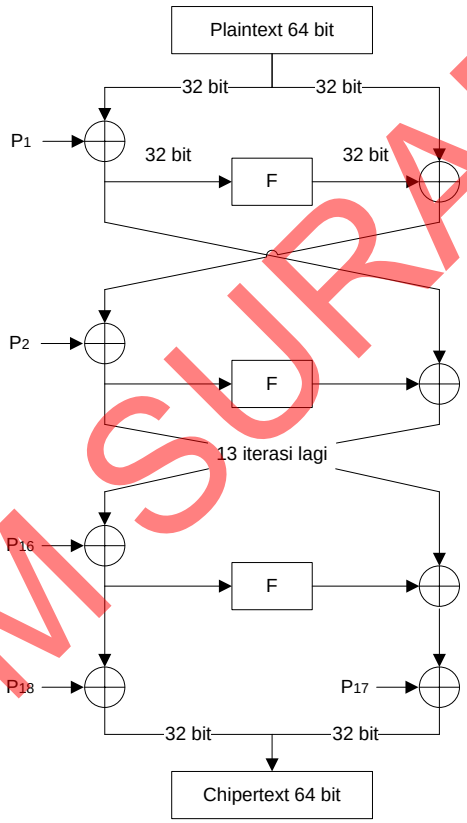
Empat S-box 32-bit masing-masing 256 entri :

$S_{1,0},S_{1,1},S_{1,2},S_{1,3},\ldots,S_{1,255}$

$S_{2,0},S_{2,1},S_{2,2},S_{2,3},\ldots,S_{2,255}$

$S_{3,0},S_{3,1},S_{3,2},S_{3,3},\ldots,S_{3,255}$

$S_{4,0},S_{4,1},S_{4,2},S_{4,3},\ldots,S_{4,255}$



Gambar 4. Blok Diagram Enkripsi Algoritma Blowfish

Blowfish merupakan sebuah jaringan Feistel (*Feistel Network*) yang mempunyai 16 putaran. Inputnya adalah (X) elemen data 64-bit. Untuk mengenkripsi yaitu :

Bagi X menjadi dua 32-bit: X_L, X_R

untuk i = 1 sampai 16

$X_L = X_L \oplus P_i$

$X_R = F(X_L) \oplus X_R$

Tukar X_L dan X_R

Tukar X_L dan X_R (batalkan penukaran terakhir)

$X_R = X_R \oplus P_{17}$

$X_L = X_L \oplus P_{18}$

Kombinasikan kembali X_L dan X_R

Fungsi F adalah sebagai berikut:

Bagi X_L, menjadi empat bagian 8-bit: *a*, *b*, *c* dan *d*

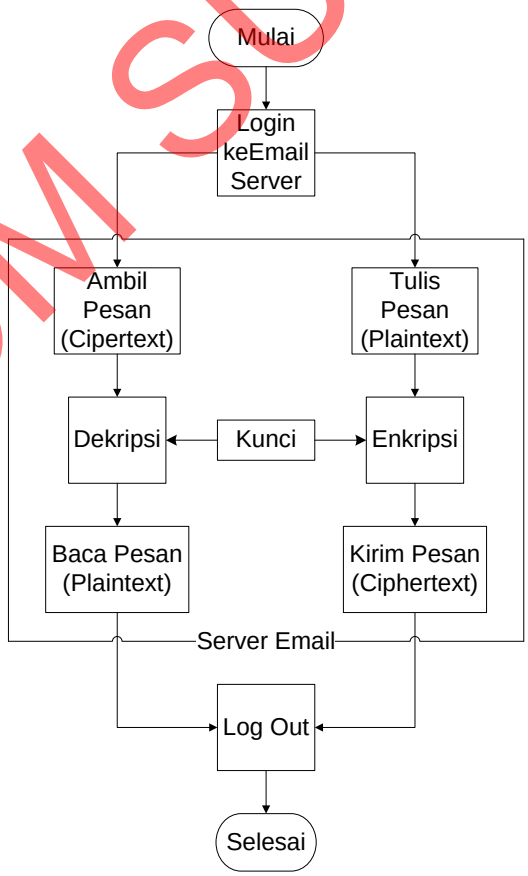
$F(X_L) = ((S_{1,a} + S_{2,b} \bmod 2^{32}) \oplus S_{3,c}) + S_{4,c} \bmod 2^{32}$

Dekripsi sama persis dengan enkripsi, kecuali $P_1, P_2, \ldots, P_{18}$ digunakan pada urutan yang terbalik.

METODE

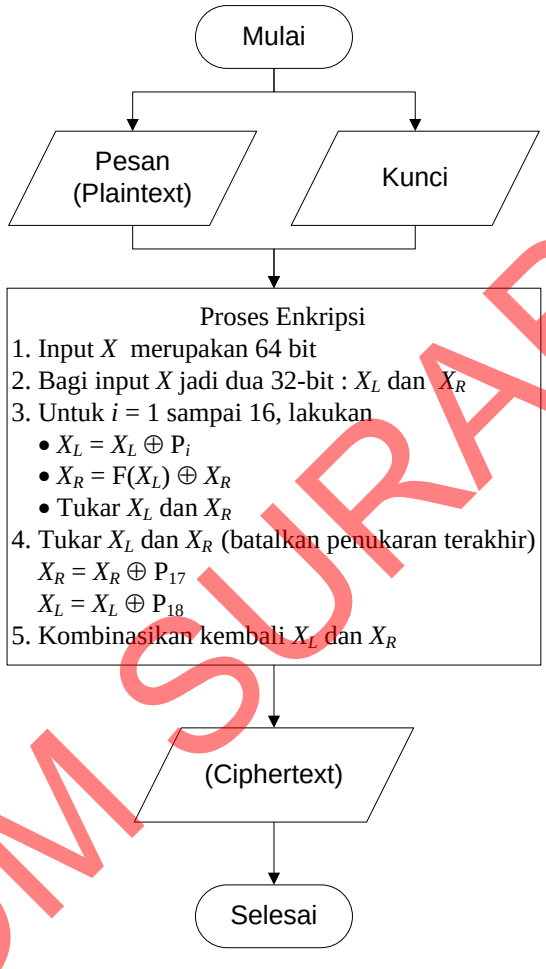
Sistem keamanan *message* email yang dirancang dan dibangun dalam penelitian ini adalah sistem keamanan yang berbasis jaringan lokal dan contoh kasus yang digunakan pada CV. Dwi Rejeki Abadi.

Sistem yang dibangun dapat menyembunyikan pesan sesungguhnya sehingga terlihat tidak berarti dan dapat menampilkan pesan sesungguhnya dengan benar sesuai dengan pesan yang terkandung. Pengguna adalah user yang sudah memiliki keanggotaan pada sebuah server email. Untuk lebih detail dapat diuraikan pada gambar 5.



Gambar 5. Diagram Alir Sistem Enkripsi dan Dekripsi Email

Dimulai dari login yang berfungsi untuk keamanan, apakah pengguna adalah user yang telah terdaftar keanggotaannya atau tidak pada server email. User dapat melakukan pengiriman atau pembacaan pesan email yang terenkripsi dengan suatu kunci tertentu secara otomatis, kunci ini ditentukan oleh kedua pihak sebelumnya dan digunakan untuk enkripsi dan dekripsi pesan email. Logout berfungsi untuk memutuskan hubungan dengan server email atau keluar.



Gambar 6. Flowchart Input dan Output Enkripsi

Gambar 6 diatas menunjukan flowchart Input dan Output dari proses enkripsi, proses dimulai dari input kunci dan input pesan(plaintext). Kunci digunakan untuk mengenkripsi pesan untuk menghasilkan output berupa chipertext, input dan output berupa karakter ascii. Untuk dekripsi sama persis dengan enkripsi, kecuali P_1, P_2, . . . , P_{18} digunakan pada urutan yang terbalik.

Enkripsi data terdiri dari iterasi fungsi sederhana sebanyak 16 kali, semua operasi adalah penambahan dan XOR pada variabel 32 bit. Enkripsi dengan Blowfish menggunakan subkunci yang besar, kunci ini harus dihitung sebelum proses enkripsi atau dekripsi data. Subkunci dihitung menggunakan algoritma Blowfish dan algoritmanya dibawah ini :

1. Inisialisasi P-array dan empat S-box secara berurutan dengan string yang tetap. String ini terdiri digit hexadesimal dari Pi.

Array P terdiri dari delapan belas 32-bit subkunci:

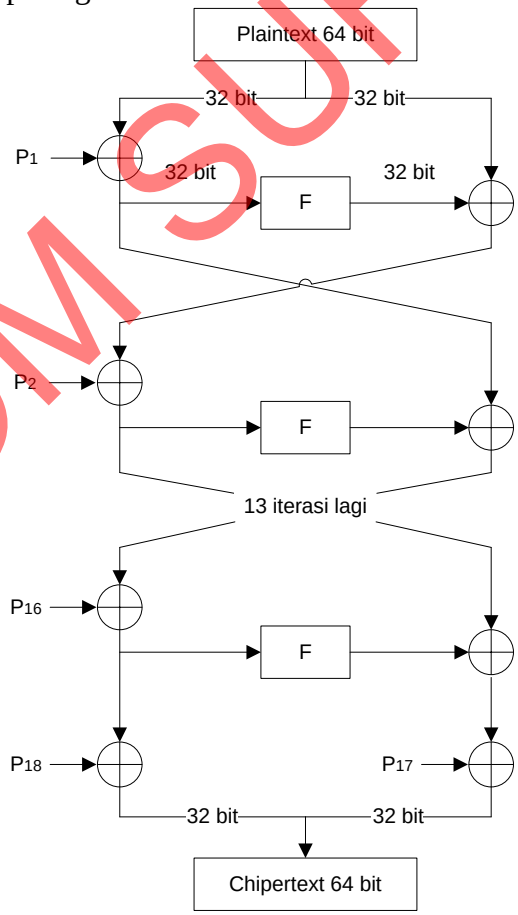
$P_1, P_2, \ldots, P_{18}$

Empat 32-bit S-box masing-masing mempunyai 256 entri:

$S_{1,0}, S_{1,1}, \ldots, S_{1,255}$
$S_{2,0}, S_{2,1}, \ldots, S_{2,255}$
$S_{3,0}, S_{3,1}, \ldots, S_{3,255}$
$S_{4,0}, S_{4,1}, \ldots, S_{4,255}$

2. XOR P_1 dengan 32 bit pertama dari kunci, Lakukan XOR P_2 dengan 32 bit kedua dari kunci dan seterusnya untuk setiap bit dari kunci (sampai P_{18}). Ulangi terhadap bit kunci sampai seluruh P-array di XOR dengan bit kunci.
3. Enkrip semua string nol dengan algoritma Blowfish dengan menggunakan subkunci seperti dijelaskan pada langkah (1) dan (2).
4. Ganti P_1 dan P_2 dengan keluaran dari langkah (3).
5. Enkrip keluaran dari langkah (3) dengan algoritma Blowfish dengan subkunci yang sudah dimodifikasi.
6. Ganti P_3 dan P_4 dengan keluaran dari langkah (5).
7. Lanjutkan proses tersebut, seluruh elemen dari P-array diganti, dan kemudian seluruh keempat S-box berurutan, dengan keluaran yang berubah secara kontinyu dari algoritma Blowfish.

Proses enkripsinya itu sendiri terdiri 16 putaran yang dapat digambarkan dalam blok diagram pada gambar 7.



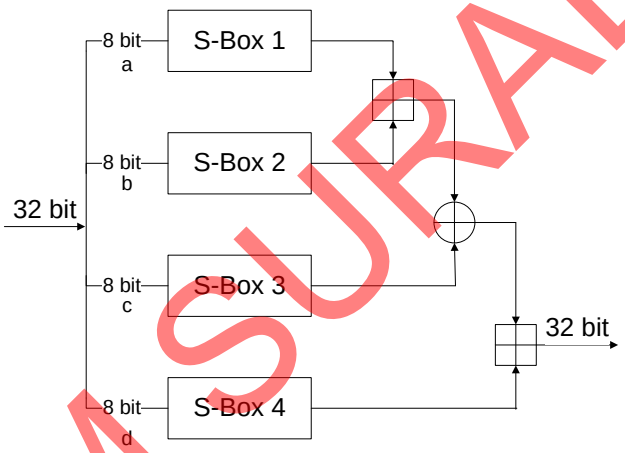
Gambar 7. Blok Diagram Enkripsi Algoritma Blowfish

Jika dijabarkan dalam langkah-langkah pseudocode akan berbentuk sebagai berikut :

1. Input X yang merupakan elemen 64 bit
2. Bagi inputan X menjadi dua 32-bit yaitu X_L dan X_R
3. Untuk i = 1 sampai 16, lakukan
   - $X_L = X_L \oplus P_i$
   - $X_R = F(X_L) \oplus X_R$
   - Tukar X_L dan X_R
4. Tukar X_L dan X_R (batalkan penukaran terakhir)
   $X_R = X_R \oplus P_{17}$
   $X_L = X_L \oplus P_{18}$
5. Kombinasikan kembali X_L dan X_R

Sedangkan fungsi F sendiri pada gambar 8 adalah sebagai berikut:

1. Bagi X_L, menjadi empat bagian 8-bit: a, b, c dan d
2. $F(X_L) = ((S_{1,a} + S_{2,b} \bmod 2^{32}) \oplus S_{3,c}) + S_{4,c} \bmod 2^{32}$



Gambar 8. Fungsi F Algoritma Blowfish

Dekripsi sama persis dengan enkripsi, kecuali P_1, P_2, . . . , P_{18} digunakan pada urutan yang terbalik.

HASIL DAN PEMBAHASAN

Tahap implementasi program merupakan suatu tahap penerapan dari analisa dan desain sistem yang telah dibuat sebelumnya. Adapun kebutuhan yang harus dipersiapkan agar program dapat diterapkan adalah kebutuhan perangkat keras maupun kebutuhan perangkat lunak.

Perangkat lunak yang digunakan dalam pembuatan aplikasi ini adalah :

1. Sistem Operasi Windows 9X/ME/2000/XP/2003.
2. Menggunakan MDaemon Mail Server.
3. Bahasa Pemrograman Visual C++ 6.0.

Perangkat keras yang digunakan dalam pembuatan aplikasi ini adalah :

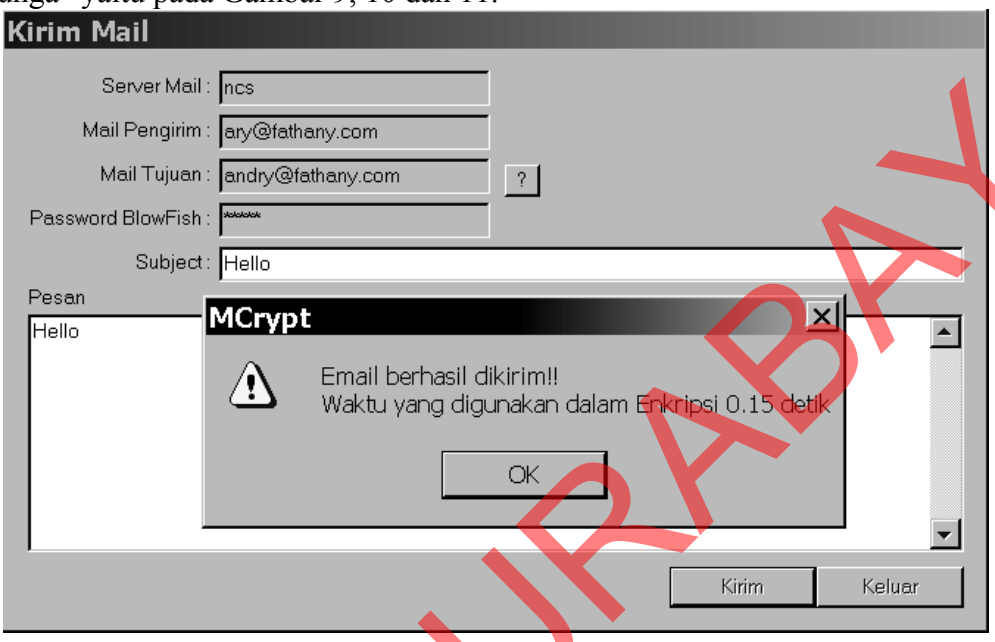
1. Prosesor dengan kecepatan 1 Ghz.
2. Memori 128 MB.
3. Harddisk 20 GB.
4. Monitor SVGA.

5. Keyboard dan Mouse.

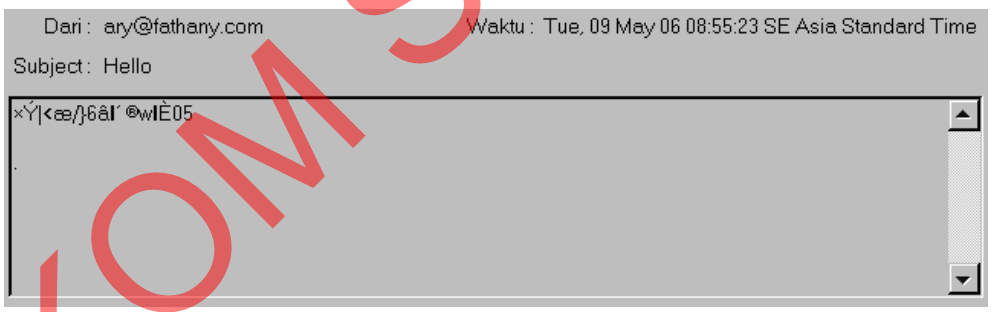
Pada tahap ini Penulis melakukan *testing* program yang telah dibuat untuk dievaluasi. Hasil yang diperoleh adalah sebagai berikut :

Ilustrasi I :

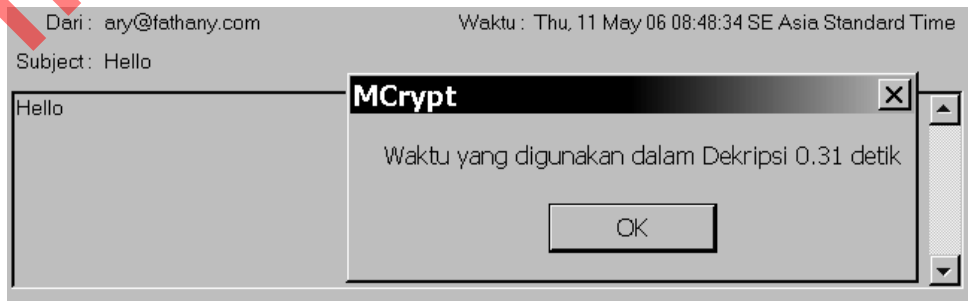
Ilustrasi pertama peneliti menggunakan pesan pendek dengan password Blowfish "bunga" yaitu pada Gambar 9, 10 dan 11.



Gambar 9. Tampilan Ilustrasi I Kirim Pesan



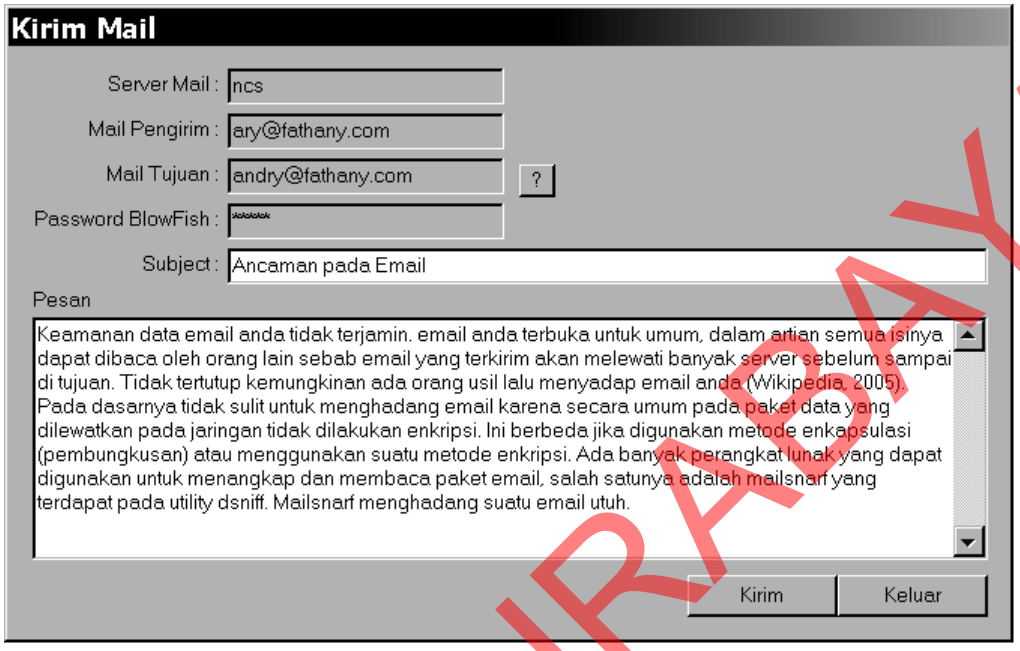
Gambar 10. Tampilan Ilustrasi I Baca Pesan Enkripsi



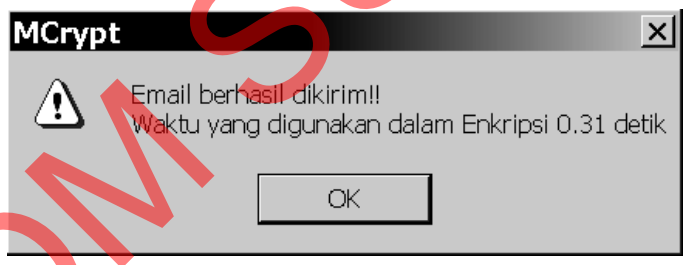
Gambar 11. Tampilan Ilustrasi I Baca Pesan

Ilustrasi II :

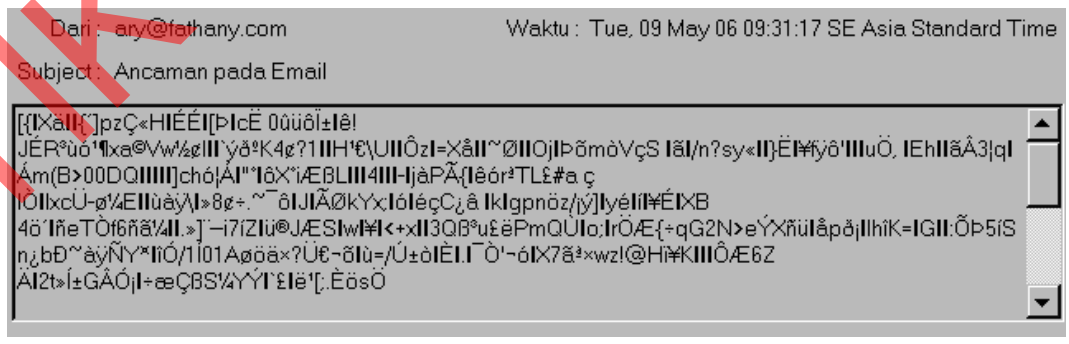
Ilustrasi kedua peneliti menggunakan pesan panjang dengan password Blowfish "bunga" yaitu pada Gambar 12, 13, 14, 15 dan 16.



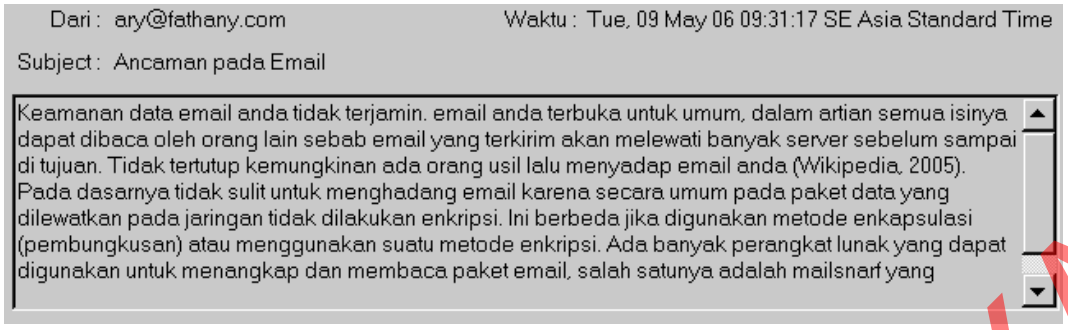
Gambar 12 Tampilan Ilustrasi II Kirim Pesan



Gambar 13. Tampilan Ilustrasi II Informasi Kirim Pesan



Gambar 14. Tampilan Ilustrasi II Baca Pesan Enkripsi



Gambar 15. Tampilan Ilustrasi II Baca Pesan

Gambar 16. Tampilan Ilustrasi II Informasi Dekripsi Pesan

Dari ilustrasi diatas dapat diketahui Enkripsi dengan algoritma Blowfish dipengaruhi panjang karakter pesan yang dikirim, waktu yang digunakan dalam dekripsi pesan lebih lama dari waktu yang digunakan dalam enkripsi pesan.

SIMPULAN

Implementasi algoritma Blowfish untuk mengenkripsi isi dari suatu email dirancang dan dibangun sebagai implementasi untuk mengatasi permasalahan keamanan pesan ketika dikirim melalui server email didalam suatu jaringan komputer. Metode Blowfish merupakan metode enkripsi yang diterapkan didalam sistem ini dengan tujuan bahwa pesan hasil enkripsi tidak dapat dengan mudah untuk dibaca oleh pengguna yang tidak berhak mengetahuinya.

Proses enkripsi dan dekripsi yang dilakukan terhadap beberapa macam jenis pesan berdasar panjang pesan mempunyai waktu eksekusi yang berbeda, pesan yang pendek mempunyai waktu yang lebih cepat dibandingkan dengan pesan yang lebih panjang dan kecepatan komputer itu sendiri untuk melakukan proses.

DAFTAR RUJUKAN

Kurniawan, A. 2002. *Pemrograman Jaringan Internet dengan Visual C++*. Jakarta: Penerbit: Elex Media Komputindo.

Scheneier, B. 1996. *Applied Cryptography-Protocols, Algorithm and Source Code in C, 2nd Edition*. New York: John Wiley & Sons.

Sembiring, J. H. 2002. *Jaringan Komputer Berbasis Linux*. Jakarta: Penerbit Elex Media Komputindo.

Stiawan, D. 2005. *Sistem Keamanan Komputer*. Jakarta: Elex Media Komputindo.

Sukmawan, B. 1998. *Keamanan Data dan Metoda Enkripsi* , Januari 1998. <bdg.centrin.net\bdg.centrin.net.id\~budskman\protek.htm>

Sukmawan, B. 2000. *Metoda Enkripsi Blowfish*, 20 Oktober 2000. <http://bdg.centrin.net.id/~budskman/blowfish.htm>

Whandoyo, N. C. 2004. *Rancang Bangun Sistem Keamanan File Menggunakan Algoritma Blowfish*. Surabaya: STIKOM.

Wikipedia. 2005. *Kriptografi*. 7 September 2005. http://id.wikipedia.org/wiki/Kriptografi>

Wikipedia. 2005. *POP3*. 6 September 2005. <http://id.wikipedia.org/wiki/POP3>

Wikipedia. 2005. *SMTP*. 8 Juli 2005. <http://id.wikipedia.org/wiki/SMTP>

Wikipedia. 2005. *Surat Elektronik*. 26 Agustus 2005. <http://id.wikipedia.org/wiki/Email>